Volume 7, Issue 1, Spring 2010 http://www.esecurity.ch/communications.html

Contents

1 Editorial

A few years ago, I published an article entitled "IT Security: In Search of the Holy Grail" in the renowned computer science magazine *Communications of the ACM* (Vol. 50, No. 2, February 2007, pp. 96–98). In this article, I advocated the design and implementation of appropriate security architectures and criticized the ongoing trend towards penetration testing and ethical hacking. I also argued that the results that can be achieved with penetration testing and ethical hacking are arbitrary and random, and hence questionable (to say the least). In the real world, we don't see ethical burglar services, and there are very legitimate reasons for their non-existence. In particular, we know from experience that every buildung can be penetrated, and hence we don't invest in the proof of this triviality. In the digital world, however, the situation is less clear and more involved. There are people who (still) think that IT systems and infrstructures can be built that cannot be penetrated. These people are routinely impressed by the results of penetration testers and ethical hackers. In the real world, external security patrol and monitoring services are used (instead of penetration testing and ethical hacking services), and such services may also be useful in the digital world. Following this line of argumentation, we are now in the process of designing external security patrol and monitoring services for the digital world, and we have preliminarily coined the term SECURITAR—an acronym derived from SECURIty avaTAR—to refer to them. We have submitted the made-up word SECURITAR to the Swiss Federal Institute of Intellectual Property for possible registration as a trademark, and we have registered the domain name `securitar.ch`. If a browser connects to `www.securitar.ch`, it is redirected to a subdirectory of `www.esecurity.ch` from where a PDF leaflet describing the basic ideas of SECURITAR can actually be downloaded (in German only). We are now in a phase in which we are looking for partner companies to bring SECURITAR and corresponding services to market. If you are interested in the topic, please drop us a note or contact us directly. We endorse and appreciate any discussion on this topic.

Anyway, I hope that you enjoy reading this issue of eSECURITY communications, and I am looking forward hearing from you and receiving your feedback, comments, or criticism in one way or another.

Rolf Oppliger
March 2010

2 News

In April 2010, eSECURITY Technologies Rolf Oppliger will move from Beethovenstrasse 10 in CH-3073 Gümligen to Breichtenstrasse 18 in CH-3074 Muri b. Bern. We hope to be fully operational again in May 2010. Please, use the new postal address to contact us after this date. All other contact information, including, for example, phone and fax numbers as well as e-mail addresses, will remain unchanged.

Earlier this year, Rolf Oppliger accepted an invitation to become an editorial board member of the *IEEE Security & Privacy* magazine,[1] which is the IEEE Computer Society's flagship publication on information security and privacy. The membership will become effective (and visible on the magazine's Web site) later this year.

3 Publications

On behalf of the International Association for Cryptologic Research (IACR), Rolf Oppliger has reviewed a book entitled "Complexity Theory and Cryptology — An Introduction to Cryptocomplexity" (Springer, 2005, ISBN 978-3-540-22147-0) and its German translation entitled "Komplexitätstheorie und Kryptologie — Eine Einführung in Kryptokomplexität" (Springer, 2008, ISBN 978-3-540-79744-9). The books are written by Jörg Rothe, who is currently a professor at the University of Düsseldorf in Germany. The books comprehensively explore the intermediate research area between modern cryptology and complexitity theory (called cryptocomplexity). It is recommended reading for anybody working in the field. The reviews are available on the IACR Books Review Web site.[2]

More recently, the slides for Rolf Oppliger's last but one book entitled "Contemporary Cryptography" have been revised and published with a Creative Commons Attribution No Derivatives (cc by-nd) 3.0 license (currently in version 1.21). The licence deed[3] and legal code[4] are electronically available. In essence, you can download and use the slides at will (e.g., to teach classes on contemporary cryptography), but you must not modify them. We hope that you agree with these licence terms and that you may accept them. Again,

[1] `http://www.computer.org/security`
[2] `http://www.iacr.org/books`
[3] `http://creativecommons.org/licenses/by-nd/3.0`
[4] `http://creativecommons.org/licenses/by-nd/3.0/legalcode`

we endorse and appreciate any feedback or comment in this matter.

4 Information Security and Privacy Books

Rolf Oppliger is currently looking into possibilities to update his book entitled "Contemporary Cryptography," and to publish it as a second edition in Artech House's information security and privacy book series (probably in 2011). If you are interested in this subject, then please feel free to volunteer as a proof reader or reviewer. Any help or contribution is appreciated.

Also, the process of contracting new authors is going on. If you are interested in writing and publishing a book in the series, then you may contact either the Series Editor (Rolf Oppliger) or a Commissioning Editors (refer to the book series' home page[5] for the coordinates of the Commissioning Editors).

5 Announcements

There are a few announcements to make regarding university lectures, courses, as well as conferences and workshops.

5.1 University Lectures

On February 22, 2010, Rolf Oppliger started this year's lecture entitled "Sicherheit in der Informationstechnik" at the University of Zürich in Switzerland. The lecture takes place annually and provides a thorough introduction to various topics related to information technology (IT) security. The topics addressed are as follows:

- Introduction
- Cryptographic foundations
- Cryptographic systems (overview)
- Authentication
- Authorization and access control models
- Software anomalies and manipluations
- Evaluation and certification
- Trusted computing
- Communication and network security
- Firewall technologies
- Cryptographic security protocols
- Intrusion detection and prevention systems
- Digital signature legislation
- PKI and identity management
- Privacy and privacy-enhancing technologies

At the end of the lecture, there is room for timely topics, such as the security of Internet banking, e-voting, and VoIP. The slides are electronically available at the lecture's home page.[6] The final exam will take place on June 7, 2010. If you are interested to attend the lecture without passing the exam, then you may also contact the secretary of the Department of Informatics at the University of Zürich.

5.2 Courses

In 2010, InfoGuard AG and CRYPTO AG will host three courses on contemporary cryptography. Four out of five days will be taught by Rolf Oppliger (on the basis of the slides mentioned in Section 3). The courses will be held in English and take place in Zug. The dates are scheduled as follows:

- May 17–May 21, 2010
- September 20–24, 2010
- November 15–19, 2010

If you are interested to attend any of these courses, then you may request a flyer from InfoGuard AG or eSECURITY Technologies Rolf Oppliger. Either company can also answer questions related to the course.

Furthermore, if you are interested to host a course on contemporary cryptography or any other topic related to IT security, then please feel free to contact eSECURITY Technologies Rolf Oppliger without any commitment. We are looking forward discussing the possibilities with you.

5.3 Conferences and Workshops

In addition to SAC 2010, WISTP 2010, and IFIP SEC 2010 (as announced in the last issue of eSECURITY communications), Rolf Oppliger will also serve as a member of the programm committee for the following international conferences and workshops that will be held this year (in chronological order):

- 4th International Conference on Information Security and Assurance (ISA 2010), India, June 3 - 5, 2010

[5] http://www.esecurity.ch/serieseditor.html

[6] http://www.esecurity.ch/Teaching/uni-zh-2009.shtml

- International Conference on Security and Cryptography (SECRYPT 2010), Athens (Greece), July 26 - 28, 2010
- 10th Annual Information Security South Africa Conference (ISSA 2010), Johannesburg (South Africa), August 2 - 4, 2010
- 5th International Conference on Systems and Networks Communications (ICSNC 2010), Nice (France), August 22 - 27, 2010
- 6th International Conference on Information Assurance and Security (IAS 2010), Atlanta (USA), August 23 - 25, 2010
- 11th International Workshop of Information Security and Applications (WISA 2010), Jeju Island (Korea), August 24 - 26, 2010
- 7th International Conference on Trust, Privacy and Security in Digital Business (TrustBus '10) held in conjunction with the 21st International Conference on Database and Expert Systems Applications (DEXA 2010), Bilbao (Spain), August 30 - September 3, 2010
- ISSE/SICHERHEIT 2010, Berlin (Germany), October 5 - 7, 2010
- International Conference on Security Technology (SecTech 2010), Cebu (Philippines), November 11 - 13, 2010
- 13th International Conference on Information Security and Cryptology (ICISC 2010), Seoul (Korea), December 1 - 3, 2010

It goes without saying that the conferences and workshops are recommended events to attend and learn more about the current state-of-the-art in cryptography and IT security.

About the Company

eSECURITY Technologies Rolf Oppliger[7] is an independent and privately owned company founded in October 1999 to provide scientific and state-of-the-art consulting, education, and engineering services related to information technology (IT) security. The company is registered in the commercial register of Bern-Mittelland (CH-035.1.023.622-7) and located in Gümligen (Switzerland). As mentioned above, it will soon move to Muri b. Bern.

[7] `http://www.esecurity.ch`